

REMARKS

The Examiner rejected claims 1-6, 9-13, and 15-19 under 35 U.S.C. 102(e) as being anticipated by Porras et al US Patent 6,321,338.

On December 7, 2004, the examiner, Mr. Massimiliano Poletto, Mr. Robert Nazzal and the undersigned conducted a telephonic interview. Discussed was claim 1. The undersigned pointed out support for the hardened redundant network feature of claim 1 and pointed out that by claiming a victim data center coupled to a network and a communication device to receive data from a plurality of monitors over a redundant network, claim 1 clearly recited a system that employed two networks. Applicant offered to define this feature of the claims by clearly pointing out in the claims that the networks were separate networks. The examiner indicated that additional consideration or search would be required. Thus, no agreement was reached.

As in the prior office action, the Examiner in the summary of this rejection indicated that only claims 1-6, 9-13, 15 and 16 and 20 were rejected over Porras. However, in the body of the rejection the examiner also rejected claims 17-19 over Porras. Thus, Applicant treats this rejection as a rejection of claims 1-6, 9-13, and 15-20.

The claims were amended to clearly distinguish over Porras.

Claim 1 for instance was amended to recite ... a control center ... that is coupled to a network... including a communication device to receive data from a plurality of monitors, dispersed through the network, with the monitors sending data collected from the network over a redundant network, the redundant network being a physically separate network from the network that the plurality of monitors collect data from. Porras does not describe at least these features of claim 1.

The examiner takes the position that Porras at Col. 8 lines 13-21 teaches "a plurality of monitors over a hardened, redundant network." Porras has no such teachings at the cited passage reproduced below, or elsewhere. Rather, Col. 8 lines 13-21 describe:

The analysis engines 22, 24 receive large volumes of events and produce smaller volumes of intrusion or suspicion reports that are then fed to the resolver 20. The resolver 20 is an expert system that receives the intrusion and suspicion reports produced by the analysis engines 22, 24 and reports produced externally by other analysis engines to which it subscribes.

There is nothing in the cite passage relied on by the examiner or elsewhere in Porras that suggests much less describes a plurality of monitors over a redundant network or "a control center including a communication device to receive data from a plurality of monitors, dispersed through the network, with the monitors sending data collected from the network over "a redundant network, with the redundant network being a physically separate network from the network that the plurality of monitors collect data from."

Rather, Porras teaches to use the network that is being monitored to transfer reports produced by the monitors among the hierarchy of monitors. See for instance, FIG. 1 and Col. 3 lines 17-65. Thus, in this architecture, if a robust attack occurs on a network that causes network congestion, the monitors in Porras may not be able to exchange reports because of the likelihood of congestion on the network that is under attack. With the claimed arrangement, the control center includes a communication device to send data collected from the network over a redundant network. The redundant network is physically a separate network from the network that the plurality of monitors collect data from thus avoiding possible network congestion caused by an attack. That is, this feature makes the central controller, the monitors and hence the architecture immune to the attack.

Moreover, the architecture of the system claimed in claim 1 is distinct from that taught by Porras. In Porras, each monitor 16 includes a resolver 20 (Col. 4 lines 55-56). The Examiner identified the resolver 20 as the central controller (Office Action page 2 paragraph 3). Accordingly, in Porras the resolver is a functional unit of the monitor, whereas in claim 1 the central controller is a distinct unit that is coupled to the plurality of monitors. Therefore, Porras neither discloses nor suggests a system that includes a central controller to coordinate thwarting attacks on a victim data center.

Accordingly claim 1 and claims 9 and 18, which generally correspond to claim 1 are distinct over Porras. Claim 18 further distinguishes since it clearly is drawn to instructions to receive data from a plurality of monitors, dispersed through a first network *** with the monitors sending data collected *** from the first network over a redundant, network, with the redundant network being a physically separate network from the network that the plurality of monitors collect data from.

Dependent claims 2-6, 10-13, 15, 16, 17 and 19 further distinguish over Porras.

For instance, claim 2 recites that the control center comprises an analysis and filtering process to identify malicious traffic and to eliminate the malicious traffic from entering the victim data center. These features are not disclosed by Porras. Porras also does not describe features of Claim 3, where the data analyzed by the control center is sampled packet traffic and/or accumulated and collected statistical information about network flows.

Although Porras discusses aspects of data collection and statistical analysis, to the extent that Porras discloses such functions as claimed (which Applicant does not concede), Porras does not perform those functions with the control center. Therefore, claims 2 and 3 serve to further distinguish over Porras. Claim 4 likewise distinguishes by reciting that the control center aggregates traffic information and coordinates measures to locate and block the sources of an attack.

Claim 5 calls for the control center being a hardened site. The examiner considers Porras as teaching this at col. 2 lines 8-10 in the discussion concerning the network entity being a virtual private network. Applicants contend that the network entity referred at Col 2 lines 8-10 is the network entity set out at Col 1 lines 45-46, which corresponds to a network forwarding device, e.g., router or switch being monitored, rather than one of the monitors disposed in the network to examine packets handled by the entity. This is confirmed by examination of FIG. 1 and Col. 3 lines 41-44 where Porras discloses network entities as distinct from monitors and as including gateways, routers, etc. Hence, Porras does not disclose a control center and does not disclose a control center being a hardened site.

The Examiner rejected claims 7-8 and 14 under 35 U.S.C. 103 as being obvious over Porras in view of Hill.

Hill does not solve any of the deficiencies in Porras noted above. Therefore, for at least the reasons discussed above these claims are also allowable over this combination of references.

Applicant has added new claims 21-27.

Claim 21 features the control center to coordinate thwarting of a denial of service attack on a victim data center *** a communication process and device to receive data from and send messages to a plurality of monitors *** over a redundant network that is a physically separate network from the network that the plurality of monitors collect data from. Porras does not disclose or suggest this feature. For this reason alone, claim 21 and its dependent claims are allowable.

Claim 21 further recites that the control center includes a process that executes on the computer system to analyze the data from the plurality of monitors *** and to send the messages to the monitors to control monitors in the network to coordinate thwarting an attack on the victim data center. This feature is also not disclosed by Porras.

Claim 22, which claims a process to select a filtering process to eliminate the malicious traffic from entering the victim data center, claim 23 claiming a process to aggregate traffic statistics to use in coordinating measures to locate and block the sources of an attack, and claim 24 claiming a process to classify attacks and determine a response based on the class of attack, all add distinct features to applicant's invention. Claim 25, which limits the classes of attack to a low-grade attack with spoofing, a low-grade attack without spoofing and a high-grade attack whether spoofing or non-spoofing also distinguishes over the reference, since Porras does not teach that the resolver classifies attacks and recognizes low-grade attack with spoofing, low-grade attack without spoofing and a high-grade attack whether spoofing or non-spoofing type of attacks. Claim 26, which recites sending requests to gateways and/or data collectors to send data back to the system pertaining to an attack and claim 27, which recites a process to send requests from the control center to gateways and/or data collectors to install filters to filter out attacking traffic are also not described.

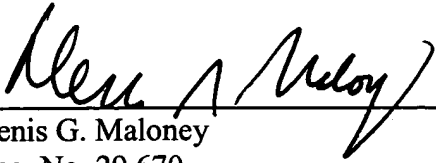
Applicant : Marinus Frans Kaashoek et al.
Serial No. : 09/931,291
Filed : August 16, 2001
Page : 12 of 12

Attorney's Docket No.: 12221-005001

Enclosed is a \$275 check for excess claim fees. Please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 12/21/04



Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110-2804
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

20985058.doc